PCT/DE 99 / 02443

BUNDESREPUBLIK DEUTSCHLAND

09 / 763271

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 17 NOV 1999
WIPO PCT

DE99/2443

EJU

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar"

am 18. August 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 L, G 09 C und H 04 K der Internationalen Patentklassifikation erhalten.

München, den 30. September 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiebinger

Aktenzeichen: 198 37 405.4

198 37 405.4 DBm 18.08.98

Beschreibung

Verfahren und Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen Schlüsselpaar.

Die Bildung eines asymmetrischen kryptographischen Schlüsselpaars ist aus [1] bekannt.

Bei diesem Verfahren wird das RSA-Verfahren zur Bildung eines kryptographischen Schlüsselpaars, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, gebildet.

Der geheime Schlüssel ist nur dem Benutzer bekannt, der öffentliche Schlüssel kann allen Teilnehmern eines Kommunikationsnetzes bekannt gemacht werden.

Bei der Erstellung einer digitalen Signatur zum Schutz der Authentizität und Integrität elektronischer Daten unterschreibt der Benutzer die Daten mit seinem geheimen Schlüssel. Die Verifikation der unterschriebenen digitalen Signatur erfolgt unter Verwendung des zu dem geheimen Schlüssels korrespondierenden öffentlichen Schlüssel, wodurch die Authentizität bzw. Integrität der digitalen Signatur von allen Kommunikationspartnern überprüft werden kann, die Zugriff auf den öffentlichen Schlüssel haben.

Die oben beschriebene sogenannte Public-Key-Technologie findet insbesondere in der digitalen Kommunikation innerhalb eines Rechnernetzes (eine vorgebbare Anzahl von Rechnereinhei-

ten, die über ein Kommunikationsnetz miteinander verbunden sind) Anwendung.

Bei dem aus [1] bekannten Verfahren ist der Schutz des geheimen Schlüssels vor unberechtigter Kenntnisnahme eines Dritten für die Sicherheit der digitalen Signatur von essentieller Bedeutung.

Aus [2] ist es bekannt, den geheimen Schlüssel auf einem externen Medium zur Speicherung von Daten, beispielsweise einer Chipkarte, einer Diskette, etc. oder auf einer Festplatte zu speichern, wobei Schlüsseldaten unter Verwendung eines persönlichen Identifizierungscodes (Personal Identification Number, PIN) oder eines Paßworts, mit dem jeweils die Schlüsseldaten verschlüsselt werden, geschützt werden. Bei Nutzung dieser externen Medien sind jedoch Zugriffe auf die lokalen Ressourcen eines Benutzers notwendig. Dies ist jedoch gerade bei einer netzorientierten Infrastruktur von Netzcomputern oder Java-Applikationen nicht gewünscht.

Unter einem Netzcomputer ist ein Rechner zu verstehen, der mit weiteren Rechnern vernetzt ist.

Unter einer Java-Applikation ist ein Programm zu verstehen, welches in der Programmiersprache Java geschriebene Programm enthält.

Somit weist das aus [2] beschriebene Verfahren den Nachteil auf, daß der geheime Schlüssel auf einem externen Medium gespeichert werden muß und somit der geheime Schlüssel vor Mißbrauch nur schwer schützbar ist.

Eine Übersicht über Hash-Funktionen ist in [3] zu finden. Unter einer Hash-Funktion ist eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfol-

ge fester Länge zugeordnet. Des weiteren können für die Hash-Funktion zusätzliche Eigenschaften gefordert werden. Eine solche zusätzliche Eigenschaft ist Kollisionsfreiheit, d.h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

Beispiele einer Hash-Funktion sind das Verfahren gemäß dem MD-2-Standard, das Verfahren gemäß dem MD-5-Standard, der Data Encryption Standard (DES), welcher ohne Verwendung eines Schlüssels durchgeführt wird, oder auch jede andere beliebige Hash-Funktion.

Ein als Verfahren nach Miller-Rabin bezeichnetes Verfahren, mit dem für eine Zahl überprüft werden kann, ob diese eine Primzahl darstellt, ist aus [4] bekannt.

Somit liegt der Erfindung das Problem zugrunde, einen geheimen Kommunikationsschlüssel zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar zu bilden, bei dem der geheime Schlüssel des asymmetrischen Schlüsselpaars nicht dauerhaft gespeichert werden muß.

Das Problem wird durch das Verfahren sowie durch die Anordnung mit den Merkmalen der unabhängigen Patentansprüche gelöst.

Bei dem Verfahren zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, wurde bei der Ermittlung des Schlüsselpaars ein vorgebbarer Startwert verwendet. Der Startwert wird einem Benutzer zur Verfügung gestellt. Der Benutzer gibt den Startwert in den Rechner ein und unter Verwendung des Startwerts wird der geheime Kommunikationsschlüssel gebildet. Der geheime Kommuni-

kationsschlüssel und der öffentliche Schlüssel bilden ein Kommunikationsschlüsselpaar.

Die Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, weist einen Prozessor auf, der derart eingerichtet ist, daß folgende Schritte durchführbar sind:

- bei der Ermittlung des Schlüsselpaars wurde ein vorgebbarer Startwert verwendet,
- der Startwert wird einem Benutzer zur Verfügung gestellt,
- der Startwert wird von dem Benutzer in den Rechner eingegeben,
- unter Verwendung des Startwerts wird der geheime Kommunikationsschlüssel gebildet, wobei der geheime Kommunikationsschlüssel und der öffentliche Schlüssel ein Kommunikationsschlüsselpaar bilden.

Ferner ist ein Eingabemittel vorgesehen zur Eingabe des Startwerts durch den Benutzer.

Durch die Erfindung wird es möglich, den geheimen Schlüssel löschen zu können, ohne auf die starke Kryptographie der Public-Key-Technologie verzichten zu müssen.

Anschaulich kann der Startwert als ein von dem Benutzer vorgegebener oder auch zentral vorgegebener persönlicher Identifikationscode (Personal Identification Number PIN) oder als Paßwort angesehen werden, den der Benutzer in den Rechner eingibt. Nach Eingabe des Paßworts bzw. der PIN wird unter Verwendung der des Paßworts bzw. der PIN als Startwert der geheime Kommunikationsschlüssel, d.h. der verglichen mit dem geheimen Schlüssel gleichlautende Schlüssel gebildet, der ein Schlüsselpaar, das Kommunikationsschlüsselpaar, gemeinsam mit dem öffentlichen Schlüssel bildet.

Auf diese Weise wird mit der Erfindung eine Verschmelzung der für den Benutzer eines üblichen Rechnernetzes bzw. eines üblichen Rechners gewohnten Paßwort-Technologie mit der starken Kryptologie erreicht, ohne daß erhebliche Anstrengungen unternommen werden müssen, um geheimes Schlüsselmaterial dauerhaft zu speichern.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

In einer Weiterbildung der Erfindung ist es vorgesehen, auf den Startwert eine Hash-Funktion anzuwenden, womit ein Wert gebildet wird, der schließlich zur Schlüsselgenerierung verwendet wird.

Weiterhin können zusätzliche Daten bei der Schlüsselgenerierung verwendet werden, die bevorzugt den Benutzer selbst charakterisieren.

Bevorzugt wird zur Bildung des kryptographischen Schlüssels das RSA-Verfahren zur Schlüsselgenerierung verwendet.

Als Hash-Funktion kann das Verfahren gemäß dem MD-5-Standard, dem MD-2-Standard oder auch dem Data Encryption Standard (DES), eingesetzt als Einweg-Funktion eingesetzt werden.

Das Kommunikationsschlüsselpaar kann sowohl zur Verschlüsselung oder zur Integritätssicherung elektronischer Daten, zur Bildung einer digitalen Signatur über elektronische Daten oder auch zur Authentifikation eines Benutzers eingesetzt werden, allgemein für eine beliebige kryptographische Operation, bei der die Public-Key-Technologie eingesetzt wird, wobei das gebildete Kommunikationsschlüsselpaar verwendet wird.

Zur Beschleunigung des Verfahrens ist es in einer Ausgestaltung vorteilhaft, bei der Bildung des geheimen Schlüssels einen Index zu speichern, der im weiteren als Beschleunigungs-

kennzahl bezeichnet wird. Mit der Beschleunigungskennzahl wird angegeben, wie oft Zahlen, ausgehend von dem Startwert, daraufhin überprüft worden sind, ob die jeweilige Zahl eine Primzahl darstellt oder nicht.

Zur Überprüfung der Eigenschaft, ob eine Zahl eine Primzahl darstellt, wird vorzugsweise das Verfahren nach Miller-Rabin eingesetzt.

Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im weiteren näher erläutert.

Es zeigen

Figur 1 ein Ablaufdiagramm, in dem die Verfahrensschritte des Ausführungsbeispiels dargestellt sind;

Figur 2 eine Skizze, in dem ein Rechnernetz mit einer Vielzahl miteinander gekoppelter Rechner dargestellt ist;

Figur 3 eine symbolische Skizze, in der die Vorgehensweise zur Ermittlung einer Primzahl ausgehend von einem Startwert dargestellt ist.

Fig.2 zeigt eine Vielzahl von Rechnern 200, 210, 220, 230, 240, 250, die über ein Kommunikationsnetz 260 miteinander verbunden sind. Jeder Rechner 200, 210, 220, 230, 240, 250 weist jeweils mehrere Eingabemittel, d.h. eine Tastatur 206, 216, 226, 236, 246, 256, eine Maus 207, 217, 227, 237, 247, 257 oder einen Scanner (nicht dargestellt) oder auch eine Kamera (nicht dargestellt) auf. Über das jeweilige Eingabemittel wird über eine Eingangs-/Ausgangsschnittstelle 201, 211, 221, 231, 241, 251 einem Speicher 202, 212, 222, 232, 242, 252 die eingegebene Information zugeführt und gespeichert. Der 202, 212, 222, 232, 242, 252 Speicher ist mit der Eingangs-/Ausgangsschnittstelle 201, 211, 221, 231, 241, 251 über einen Bus 204, 214, 224, 234, 244, 254 verbunden. Ebenso

mit dem Bus 204, 214, 224, 234, 244, 254 verbunden ist ein Prozessor 203, 213, 223, 233, 243, 253, der derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchführbar sind.

Die Rechner 200, 210, 220, 230, 240, 250 kommunizieren über das Kommunikationsnetz 260 gemäß dem Transport Control Protocol/Internet Protocol (TCP/IP).

Ferner ist in dem Kommunikationsnetz 260 eine Zertifizierungseinheit 270 vorgesehen, mit der für jeweils einen öffentlichen Schlüssel ein Zertifikat ausgestellt wird, so daß der öffentliche Schlüssel vertrauenswürdig ist für eine Kommunikation auf der Basis der Public-Key-Technologie.

Ein Benutzer 280 gibt in einen ersten Rechner 200 ein beliebiges vorgebbares Wort (PIN, Paßwort), welches nur dem Benutzer bekannt ist, ein (Schritt 101, vgl. **Fig.1**).

Von dem ersten Rechner 200 wird gemäß dem RSA-Verfahren ein asymmetrisches kryptographisches Schlüsselpaar generiert, wie im folgenden beschrieben.

Der von dem Benutzer 280 eingegebene Wert 102 sowie Zusatzdaten 103, die den Benutzer 280 charakterisieren, zum Beispiel Benutzername, Personalnummer, Terminal-Adresse, etc. werden einer Hash-Funktion zugeführt (Schritt 104).

Eine Übersicht über Hash-Funktionen ist in [3] zu finden. Unter einer Hash-Funktion ist eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren können für die Hash-Funktion zusätzliche Eigenschaften gefordert werden. Eine solche zusätzliche Eigenschaft ist Kollisionsfreiheit, d.h. es darf nicht möglich sein, zwei verschiedene Eingangszei-

chenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

Beispiele einer Hash-Funktion sind das Verfahren gemäß dem MD-2-Standard, das Verfahren gemäß dem MD-5-Standard, der Data Encryption Standard (DES), welcher ohne Verwendung eines Schlüssels durchgeführt wird, oder auch jede andere beliebige Hash-Funktion.

Der durch die Hash-Funktion gebildete Wert wird als Basiswert BW zur Bildung zweier Primzahlen verwendet, wie in **Fig.3** symbolisch dargestellt ist.

Wie in **Fig.3** dargestellt, wird ausgehend von dem Basiswert BW jeweils für einen Wert Wi (i = 1, ..., n) in einem iterativen Verfahren überprüft, ob der jeweilige Wert eine Primzahl darstellt oder nicht (Schritt 301).

Als Verfahren zur Überprüfung der Eigenschaft Prim für eine Zahl wird das Verfahren gemäß Miller-Rabin eingesetzt, welches in [4] beschrieben ist.

Wird für eine Zahl festgestellt, daß die Zahl keine Primzahl ist, so wird die Zahl um einen vorgebbaren Wert, vorzugsweise um den Wert 2 erhöht (Schritt 302) und der Test auf die Eigenschaft „Prim" wird wiederholt (Schritt 301). Dieses Vorgehen wird solange wiederholt, bis zwei Primzahlen, eine erste Primzahl p und eine zweite Primzahl q ermittelt worden sind.

Als Index wird eine Zahl bezeichnet, mit der angegeben wird, wie oft ausgehend von dem Basiswert PW die Zahl um den vorgegebenen Wert erhöht werden muß, bis man zu der ersten Primzahl p bzw. zu der zweiten Primzahl q gelangt.

Ergebnis des in **Fig.3** dargestellten Verfahrens sind zwei Primzahlen p und q, die zur Schlüsselgenerierung gemäß dem RSA-Verfahren (Schritt 105) eingesetzt werden.

Die Primzahlen p und q weisen üblicherweise eine Länge mehrerer 100 Bit auf.

Aus den Primzahlen p und q wird ein Modulus n gemäß folgender Vorschrift gebildet:

$$n = p * q. \qquad (1)$$

Ferner wird eine Zwischengröße $\varphi(n)$ gemäß folgender Vorschrift gebildet:

$$\varphi(n) = (p-1) * (q-1). \qquad (2)$$

Ein geheimer Schlüssel d wird nun derart gewählt, daß der geheime Schlüssel d teilerfremd zu $\varphi(n)$ ist. Ein öffentlicher Schlüssel e wird derart bestimmt, daß folgende Vorschrift erfüllt ist:

$$e * d \text{ mop } \varphi(n) = 1. \qquad (3)$$

Der Wert d ist der geheime Schlüssel und darf keinem Dritten bekannt gemacht werden.

Somit ist durch die Schlüsselgenerierung (Schritt 105) ein privater Schlüssel d (Schritt 106) und ein öffentlicher Schlüssel e (Schritt 107) gebildet worden.

Die beiden Schlüssel d, e bilden ein zueinander korrespondierendes kryptographisches Schlüsselpaar, welches für eine beliebige kryptographische Operation, d.h. zur Verschlüsselung, zur Entschlüsselung oder auch zur digitalen Signatur oder zur Authentifikation eingesetzt wird (Schritt 108).

Nach Bildung des Schlüsselpaares d, e gemäß dem oben beschriebenen Verfahren wird der geheime Schlüssel d gelöscht.

Der öffentliche Schlüssel e wird der Zertifizierungsinstanz 280 zugeführt. Von der Zertifizierungsinstanz 280 wird ein Zertifikat Certe über den öffentlichen Schlüssel e gebildet und das Zertifikat Certe des öffentlichen Schlüssels e wird in einem öffentlich zugänglichen Verzeichnis 290 gespeichert.

Somit kann jeder Kommunikationsteilnehmer in dem Kommunikationsnetz 280 auf den öffentlichen Schlüssel e über das Zertifikat Certe des öffentlichen Schlüssels e zugreifen.

Der geheime, zu dem öffentlichen Schlüssel e korrespondierende Schlüssel d ist in dem ersten Rechner 200 gelöscht.

Jedesmal, wenn der Benutzer 280 auf der Basis des Schlüsselpaares eine Kommunikation beginnen will, bzw. eine kryptographische Operation unter Verwendung eines solchen Schlüsselpaares durchführen will, gibt der Benutzer 208 in den ersten Rechner 200 seinen Startwert (PIN, Paßwort) ein und der Startwert 102 wird wie oben beschrieben wiederum mit Zusatzdaten 103 versehen, einer Hash-Funktion unterzogen (Schritt 104) und es werden entweder ausgehend von dem Basiswert BW zwei Primzahlen p und q ermittelt oder es wird ein gespeicherter Index, wie oben beschrieben, ausgelesen oder ebenfalls von dem Benutzer 280 eingegeben und daraus wird ein geheimer Kommunikationsschlüssel gebildet, der dem geheimen, zuvor gebildeten jedoch wieder gelöschten Schlüssel d entspricht.

Auf diese Weise ist ein Kommunikationsschlüsselpaar gebildet worden, welches den geheimen Kommunikationsschlüssel sowie den korrespondierenden öffentlichen Schlüssel e umfaßt. Damit kann jeweils für eine Kommunikationssitzung von einem Benutzer aktuell der geheime Kommunikationsschlüssel erzeugt werden, womit es möglich ist, starke Public-Key-Technologie einzusetzen, ohne den geheimen Schlüssel auf einer Chipkarte speichern zu müssen.

Das somit gebildete Kommunikationsschlüsselpaar d, e wird verwendet zur Verschlüsselung von Klartext 109 mit dem öffentlichen Schlüssel e und der Entschlüsselung der elektronischen, verschlüsselten Daten 110 mit dem geheimen Kommunikationsschlüssel.

Die Verarbeitung von Klartext 109, d.h. für jedermann lesbare elektronische Daten 109 sowie verschlüsselte elektronische Daten 110 sind in **Fig.1** symbolisch dargestellt, wobei die Kommunikationsrichtung jeweils durch einen Pfeil hin bzw. von dem Block, welcher eine kryptographische Operation 108 darstellt, beschreibt.

Die Verschlüsselung bzw. Entschlüsselung erfolgt gemäß folgenden Vorschriften:

$$m^e \bmod n = c, \qquad (4)$$

wobei mit

- m eine Menge von 512 Bit elektronischer Daten 109, die es zu verschlüsseln gilt,
- c verschlüsselte elektronische Daten 110,

bezeichnet werden.

Die Entschlüsselung der verschlüsselten elektronischen Daten c erfolgt gemäß folgender Vorschrift:

$$m = c^d \bmod n. \qquad (5)$$

Im weiteren werden einige Alternativen des oben dargestellten Ausführungsbeispiels erläutert:

Das Verfahren kann sowohl zur Verschlüsselung als auch zur Integritätssicherung oder auch zur digitalen Unterschrift elektronischer Daten eingesetzt werden.

Ferner kann die Erfindung im Bereich sicherer elektronischer Mail-Systeme eingesetzt werden.

Der Startwert 102 muß bei der Generierung des Schlüsselpaars zu Beginn des Verfahrens nicht unbedingt von dem Benutzer eingegeben werden, sondern er kann auch von einer zentralen Einheit, welche das Schlüsselpaar generiert, dem Benutzer vorgegeben werden.

Somit hat sich der Benutzer lediglich ein Paßwort bzw. eine PIN zu merken und es ist nicht mehr erforderlich, einen geheimen kryptographischen Schlüssel sicher zu speichern, beispielsweise auf einer Chipkarte, was mit entsprechenden Risiken und mit erheblichem Aufwand verbunden ist.

Anstelle einer Hash-Funktion kann im Rahmen der Erfindung jede beliebige Einwegfunktion eingesetzt werden.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert.

[1] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, S. 79 - 85, 1993

[2] D. Longley und M. Shain, Data & Computer Security, Dictionary of standards concepts and terms, Stockton Press, ISBN 0-333-42935-4, S. 317, 1987

[3] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, S. 68 - 73, 1993

[4] A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN 0-8493-8523-7, S. 138 - 140, 1997

Patentansprüche

1. Verfahren zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, durch einen Rechner,

a) bei dem bei der Ermittlung des Schlüsselpaars ein vorgebbarer Startwert verwendet wurde,

b) bei dem der Startwert einem Benutzer zur Verfügung gestellt wird,

c) bei dem der Benutzer den Startwert in den Rechner eingibt

d) bei dem unter Verwendung des Startwerts der geheime Kommunikationsschlüssel gebildet wird, wobei der geheime Kommunikationsschlüssel und der öffentliche Schlüssel ein asymmetrisches kryptographisches Kommunikationsschlüsselpaar bilden.

2. Verfahren nach Anspruch 1,
bei dem der Startwert einer Hash-Funktion zugeführt wird und der durch die Hash-Funktion gebildete Wert bei der Ermittlung des Schlüsselpaars sowie des Kommunikationsschlüsselpaars verwendet wird.

3. Verfahren nach Anspruch 1 oder 2,
bei dem bei der Bildung des Schlüsselpaars und des Kommunikationsschlüsselpaars Zusatzdaten, die den Benutzer charakterisieren, verwendet werden.

4. Verfahren nach einem der Ansprüche 1 bis 3,
- bei dem ausgehend von dem Startwert eine Primzahl ermittelt wird, wobei jeweils in einem iterativen Verfahren solange daraufhin geprüft wird, ob die jeweils überprüfte Zahl eine Primzahl ist und wenn dies der Fall ist, ein Index gespeichert wird, mit dem eine Anzahl von Zahlen bezeichnet wird,

die auf ihre Eigenschaft hin, ob sie eine Primzahl sind, überprüft worden sind, gespeichert wird,
- sonst eine weitere Zahl ausgehend von der überprüften Zahl ausgewählt wird und der Index um eine vorgegebene Zahl erhöht wird,
- bei dem nach der Bildung des Kommunikationsschlüsselpaars die verwendete Primzahl gelöscht wird,
- bei dem bei der neuen Bildung eines Kommunikationsschlüsselpaars jeweils der Index und der Startwert verwendet werden zur Bildung des geheimen Kommunikationsschlüssels.

5. Verfahren nach Anspruch 4,
bei dem der Test, ob eine Zahl eine Primzahl ist, gemäß dem Verfahren nach Miller-Rabin erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem die Schlüssel gemäß dem RSA-Verfahren gebildet werden.

7. Verfahren nach einem der Ansprüche 2 bis 6,
bei dem die Hash-Funktion eines der folgenden Verfahren ist:
- MD-5-Verfahren,
- MD-2-Verfahren,
- das Verfahren gemäß dem Data Encryption Standard (DES) als Einweg-Funktion.

8. Verfahren nach einem der Ansprüche 1 bis 7,
eingesetzt zur Verschlüsselung elektronischer Daten mit dem geheimen Kommunikationsschlüssel.

9. Verfahren nach einem der Ansprüche 1 bis 7,
eingesetzt zur Bildung einer digitalen Signatur über elektronische Daten unter Verwendung des geheimen Kommunikationsschlüssels.

10. Verfahren nach einem der Ansprüche 1 bis 7,

eingesetzt zur Authentifikation unter Verwendung des geheimen Kommunikationsschlüssels.

11. Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, mit einem Prozessor, der derart eingerichtet ist, daß folgende Schritte durchführbar sind:

- das Schlüsselpaar wurde unter Verwendung eines vorgebbaren Startwerts ermittelt,
- der Startwert wird einem Benutzer zur Verfügung gestellt,
- der Startwert wird von dem Benutzer in den Rechner eingegeben,
- unter Verwendung des Startwerts wird der geheime Kommunikationsschlüssel gebildet, wobei der geheime Kommunikationsschlüssel und der öffentliche Schlüssel ein Kommunikationsschlüsselpaar bilden, und

mit einem Eingabemittel zur Eingabe des Startwerts durch den Benutzer.

12. Anordnung nach Anspruch 11,
bei der der Prozessor derart eingerichtet ist, daß der Startwert einer Hash-Funktion zugeführt wird und der durch die Hash-Funktion gebildete Wert bei der Ermittlung des Schlüsselpaars sowie des Kommunikationsschlüsselpaars verwendet wird.

13. Anordnung nach Anspruch 11 oder 12,
bei der der Prozessor derart eingerichtet ist, daß bei der Bildung des Schlüsselpaars und des Kommunikationsschlüsselpaars Zusatzdaten, die den Benutzer charakterisieren, verwendet werden.

14. Anordnung nach einem der Ansprüche 11 bis 13,
bei der der Prozessor derart eingerichtet ist, daß

- ausgehend von dem Startwert eine Primzahl ermittelt wird, wobei jeweils in einem iterativen Verfahren solange daraufhin geprüft wird, ob die jeweils überprüfte Zahl eine Primzahl ist und wenn dies der Fall ist, ein Index gespeichert wird, mit dem eine Anzahl von Zahlen bezeichnet wird, die auf ihre Eigenschaft hin, ob sie eine Primzahl sind, überprüft worden sind, gespeichert wird,
- sonst eine weitere Zahl ausgehend von der überprüften Zahl ausgewählt wird und der Index um eine vorgegebene Zahl erhöht wird,
- nach der Bildung des Kommunikationsschlüsselpaars die verwendete Primzahl gelöscht wird,
- bei der neuen Bildung eines Kommunikationsschlüsselpaars jeweils der Index und der Startwert verwendet werden zur Bildung des geheimen Kommunikationsschlüssels.

15. Anordnung nach Anspruch 14,
bei der der Prozessor derart eingerichtet ist, daß der Test, ob eine Zahl eine Primzahl ist, gemäß dem Verfahren nach Miller-Rabin erfolgt.

16. Anordnung nach einem der Ansprüche 11 bis 15,
bei der der Prozessor derart eingerichtet ist, daß die Schlüssel gemäß dem RSA-Verfahren gebildet werden.

17. Anordnung nach einem der Ansprüche 12 bis 16,
bei der der Prozessor derart eingerichtet ist, daß die Hash-Funktion eines der folgenden Verfahren ist:
- MD-5-Verfahren,
- MD-2-Verfahren,
- das Verfahren gemäß dem Data Encryption Standard (DES) als Einweg-Funktion.

18. Anordnung nach einem der Ansprüche 11 bis 17,
eingesetzt zur Verschlüsselung elektronischer Daten mit dem geheimen Kommunikationsschlüssel.

19. Anordnung nach einem der Ansprüche 11 bis 17, eingesetzt zur Bildung einer digitalen Signatur über elektronische Daten unter Verwendung des geheimen Kommunikationsschlüssels.

20. Anordnung nach einem der Ansprüche 11 bis 17, eingesetzt zur Authentifikation unter Verwendung des geheimen Kommunikationsschlüssels.

Zusammenfassung

Verfahren und Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar

Nachdem ein Schlüsselpaar mit einem öffentlichen Schlüssel und einem korrespondierenden geheimen Schlüssel ausgehend von einem Startwert ermittelt wurde, wird der Startwert einem Benutzer zur Verfügung gestellt. Der geheime Schlüssel kann gelöscht werden. Wenn der Benutzer eine auf der Public-Key-Technologie basierende kryptographische Operation durchführen möchte, gibt der Benutzer den Startwert in einen Rechner ein und unter Verwendung des Startwerts wird ein geheimer Kommunikationsschlüssel gebildet, der dem zuvor gebildeten, seitdem gelöschten geheimen Schlüssel entspricht.

Sign. Figur 1

FIG 1

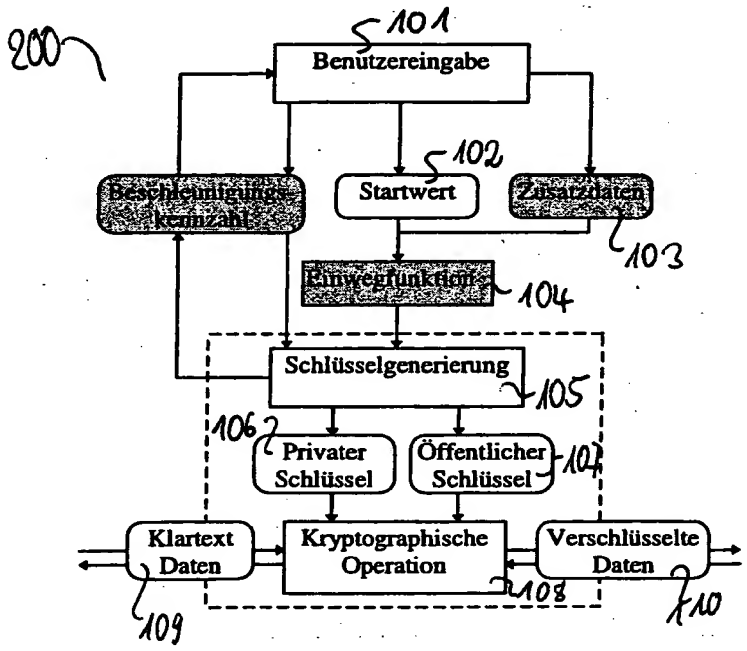

200
101
Benutzereingabe
102
Startwert
Zusatzdaten
103
Einwegfunktion
104
Schlüsselgenerierung
105
106
Privater Schlüssel
Öffentlicher Schlüssel
Klartext Daten
Kryptographische Operation
Verschlüsselte Daten
108
109
110

FIG 2

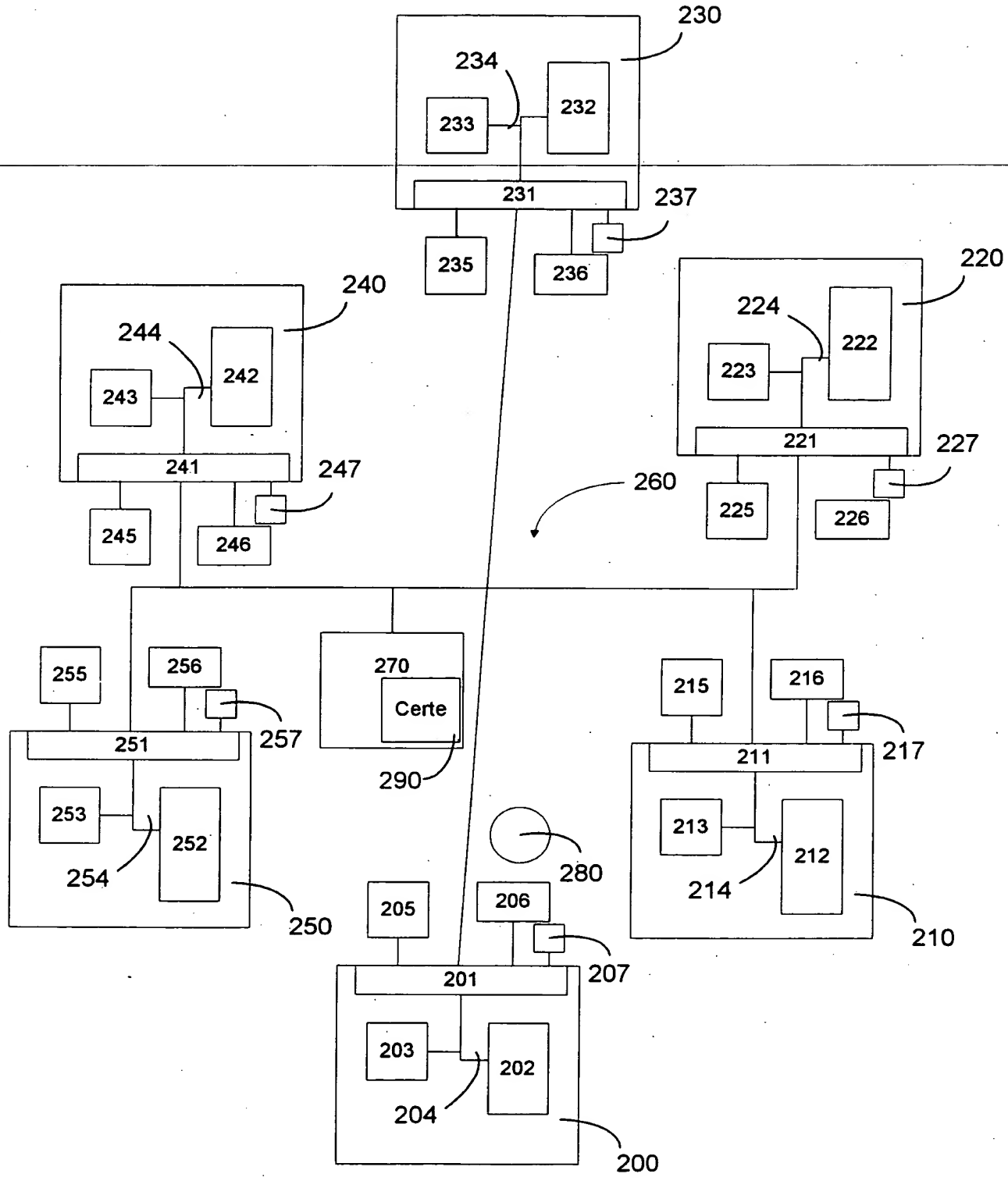
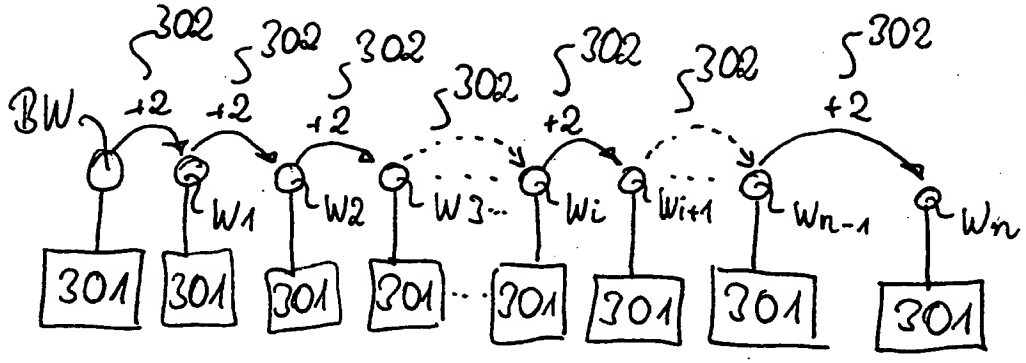

230
234
233
232
231
237
235
236
240
244
243
242
241
247
245
246
220
224
223
222
221
227
225
226
260
270
Certe
290
255
256
257
251
253
252
254
250
215
216
217
211
213
212
214
210
280
205
206
207
201
203
202
204
200

FIG 3



⇓

P1 9